Cyber Security on Nutanix at Nutanix

Brandon.Gagliardi@Nutanix.com

2019

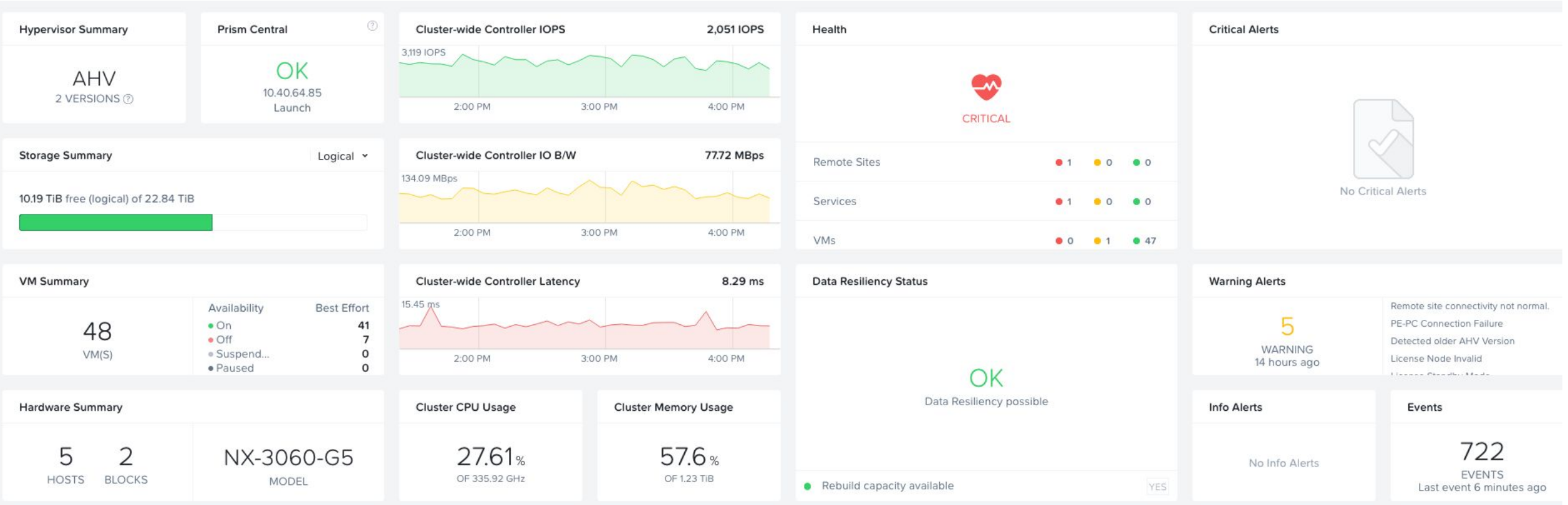
My Story

- Brandon Gagliardi
- Sr. Security Engineer

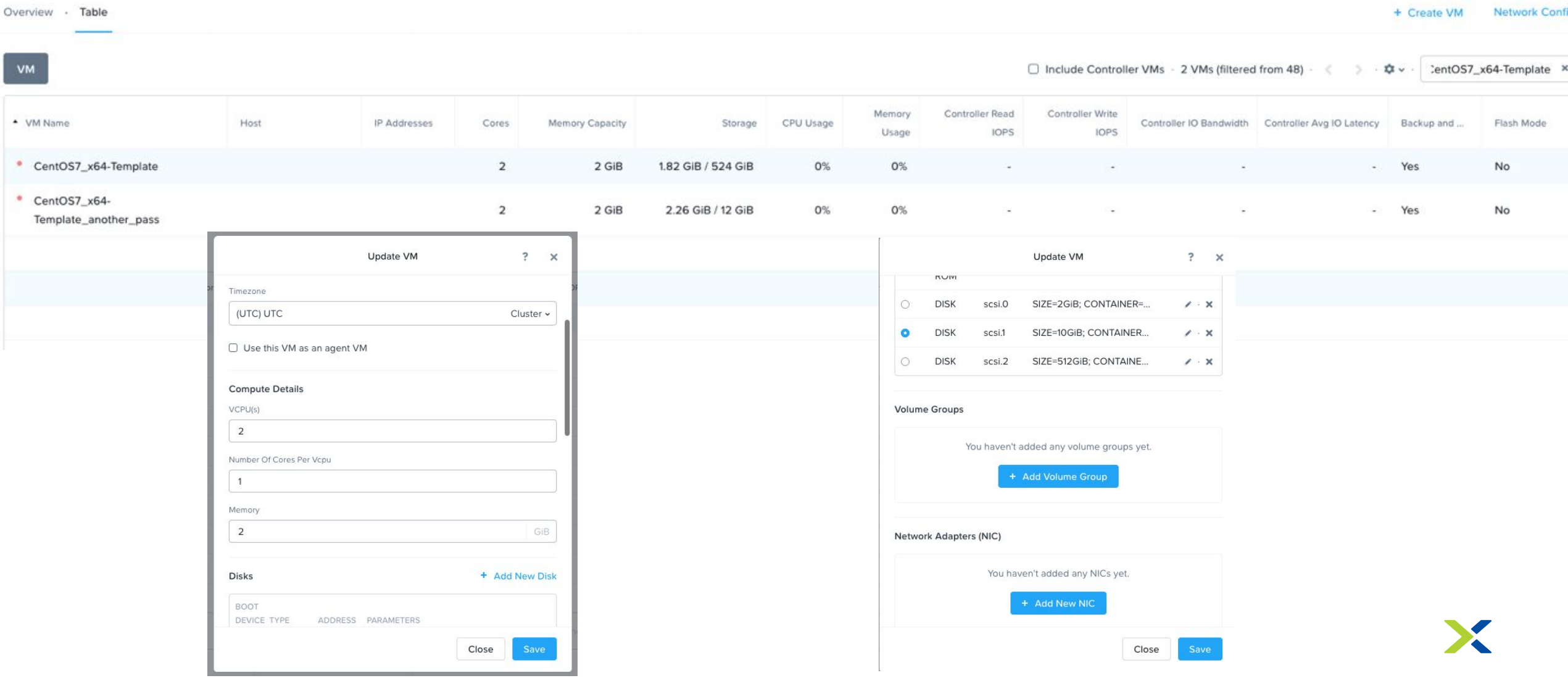
My 1st Week at Nutanix

- Drink our own champagne.
- Lean IT team.
- Major deliverables in a short time.

”Here’s your home page where you can monitor resources” – Platform team



“…Here’s The Template – This is your environment.”



Infrastructure Created in Minutes for Splunk

- First workload on Nutanix for Corp Cyber Security
- 7 VM’s
- Unique allocations of vCPU & memory per server based on Splunk best practices
- Whole environment stood up in 30minutes.
- (BTW – Dedicated vCPU’s.)

Environment Unexpected Growth

90GiB/day	4 Nodes	August 2017
200GiB/day	4 Nodes	December 2017*
500GiB/day	8 Nodes	April 2018
1TiB/day	12 Nodes	October 2018

Fun Stuff Happened Along The Way

What happened to my node? Doh!

Problems Don’t Occur When It’s Convenient

The alert condition for 'DMC Alert - Critical System Physical Memory Usage' was triggered.

Alert: DMC Alert - Critical System Physical Memory Usage

View results in Splunk

Instance	Memory used (%)	Memory used (MB)	Physical memory installed (MB)
drt-itsec-indexer-prod-2.corp.nutanix.com	95.0	22722.438	23913.102

The alert condition for 'DMC Alert - Search Peer Not Responding' was triggered.

Alert: DMC Alert - Search Peer Not Responding

View results in Splunk

Instance	Status
drt-itsec-indexer-prod-1.corp.nutanix.com:8089	Down
drt-itsec-universalforwarder-prod-1.corp.nutanix.com:8089	Down

Onboarded 30 New Security Analysts Concurrent Searches Went Up

The alert condition for 'DMC Alert - Critical System Physical Memory Usage' was triggered.

Alert: DMC Alert - Critical System Physical Memory Usage

View results in Splunk

Instance	Memory used (%)	Memory used (MB)	Physical memory installed (MB)
drt-itsec-indexer-prod-2.corp.nutanix.com	95.0	22722.438	23913.102

The alert condition for 'DMC Alert - Search Peer Not Responding' was triggered.

Alert: DMC Alert - Search Peer Not Responding

View results in Splunk

Instance	Status
drt-itsec-indexer-prod-1.corp.nutanix.com:8089	Down
drt-itsec-universalforwarder-prod-1.corp.nutanix.com:8089	Down

Data Center Migrations
Fluxes in Firewall Data (+50% Daily Ingest Spikes)

The alert condition for 'DMC Alert - Near Critical Disk Usage' was triggered.

Alert: DMC Alert - Near Critical Disk Usage

View results in Splunk

Instance	Mount Point	File System Type	Capacity (GB)	Usage (GB)	Usage (%)
drt-itsec-indexer-prod-1.corp.nutanix.com	/data	xfs	7095.48	6522.44	91
drt-itsec-indexer-prod-2.corp.nutanix.com	/data	xfs	7095.48	6418.80	90
drt-itsec-indexer-prod-3.corp.nutanix.com	/data	xfs	6072.00	5564.31	91

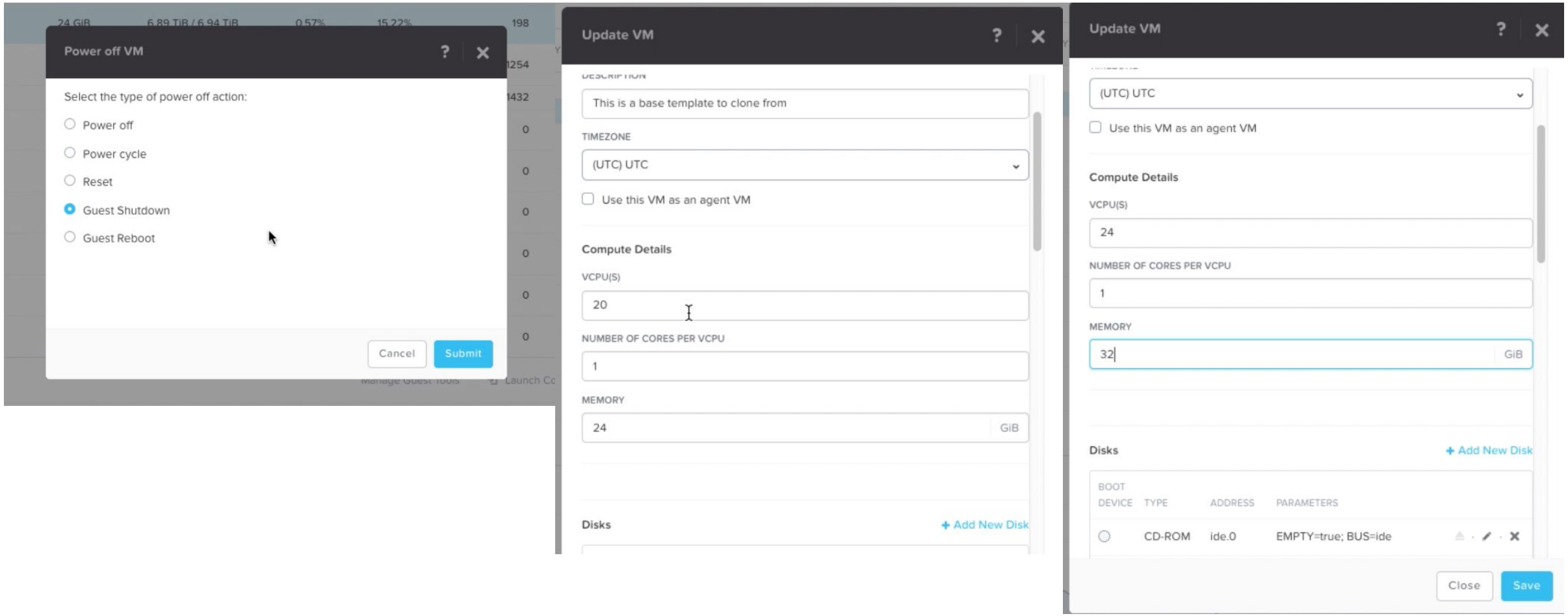
Time to Remediate and Validate Problem Start to Finish w/ Distractions: Less than 15 Minutes

Overview · Table

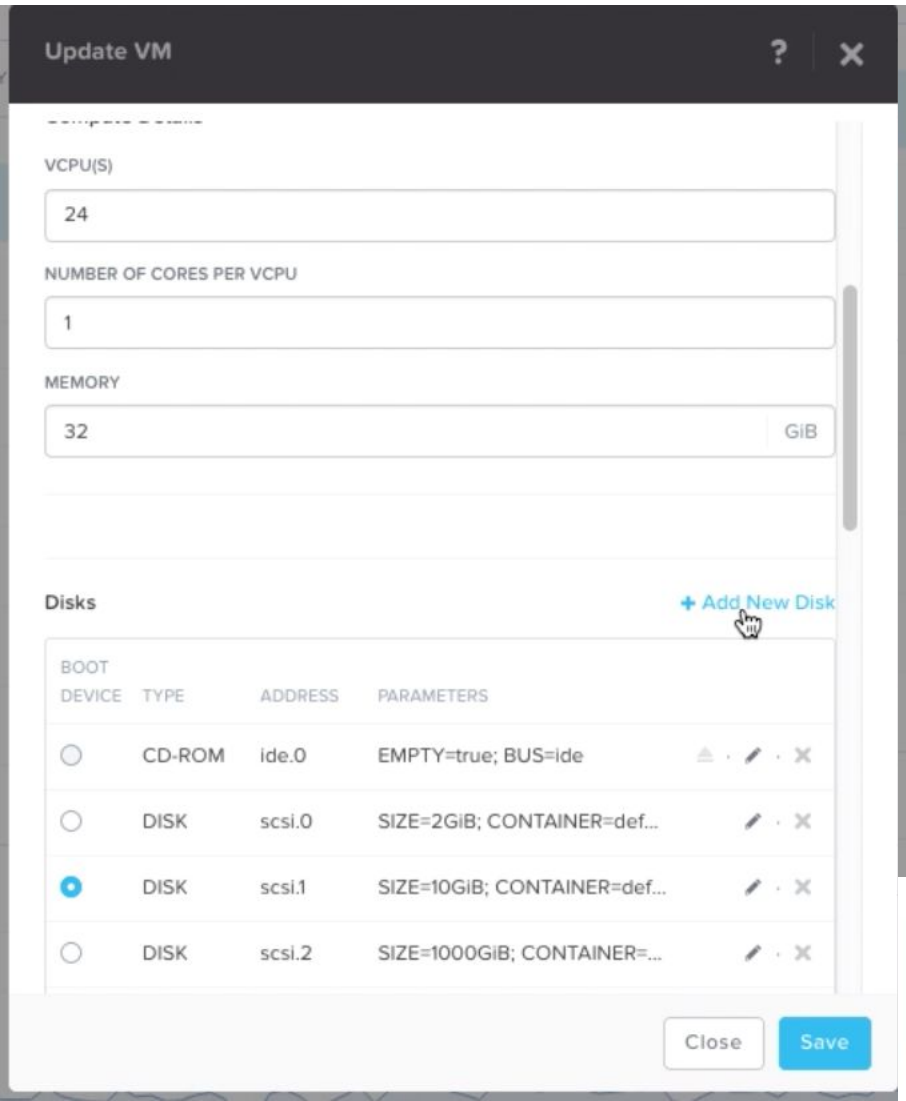
VM

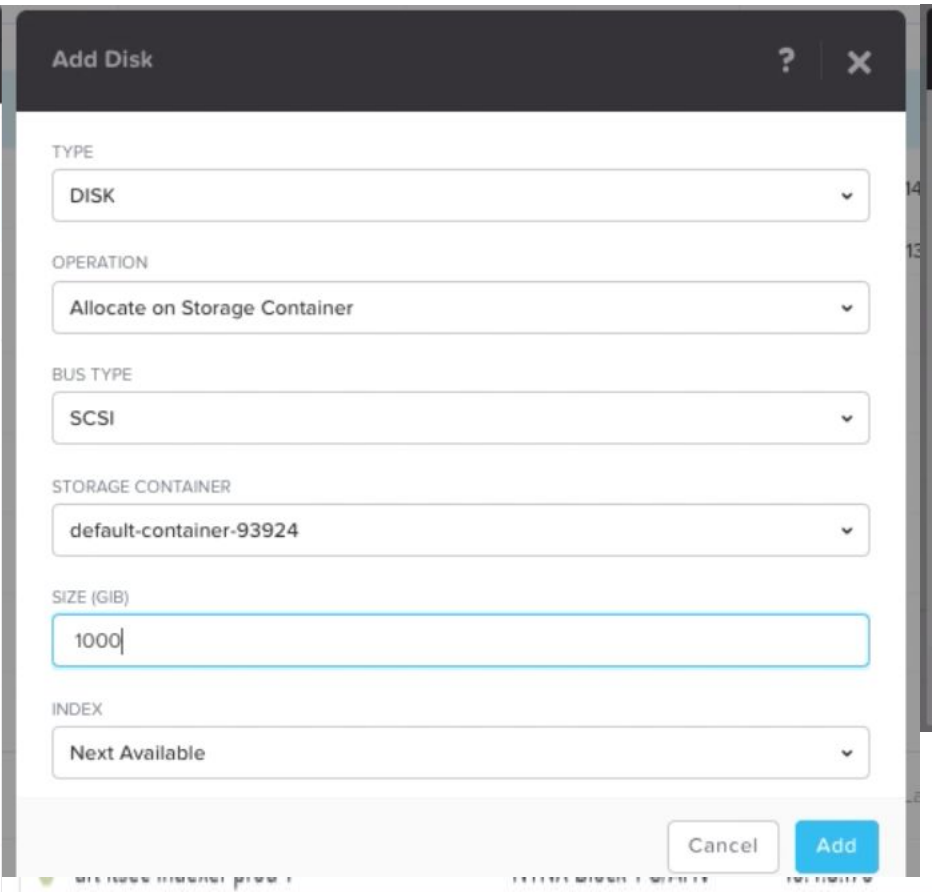
VM NAME	HOST	IP ADDRESSES	CORES	MEMORY CAPACITY	STORAGE	CPU USAGE	MEMORY USAGE
drt-itsec-indexer-prod-1	NTNX-Block-1-C/AHV	10.4.8.170	20	24 GiB	6.93 TiB / 6.94 TiB	1.09%	99.93%
drt-itsec-indexer-prod-2	NTNX-18SM6F140180-C/AHV	10.4.8.171	20	24 GiB	6.89 TiB / 6.94 TiB	81.13%	99.31%
drt-itsec-indexer-prod-3	NTNX-18SM6F140180-A/AHV	10.4.204.24	20	24 GiB	5.69 TiB / 5.94 TiB	92.85%	97.42%
drt-itsec-indexer-prod-4	NTNX-Block-1-A/AHV	10.4.204.25	20	24 GiB	5.13 TiB / 5.94 TiB	93.04%	98.25%

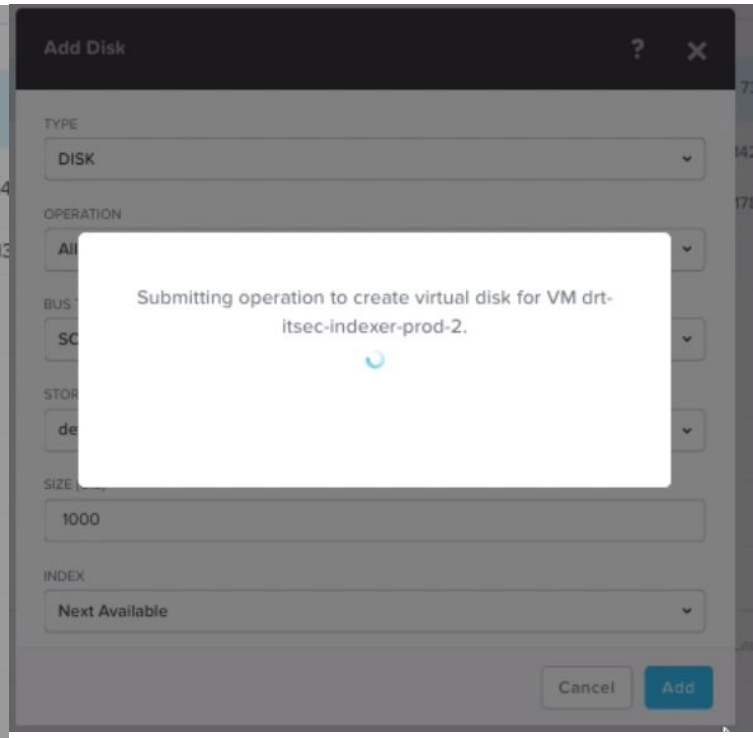
Shut VM Down and Give it More Power

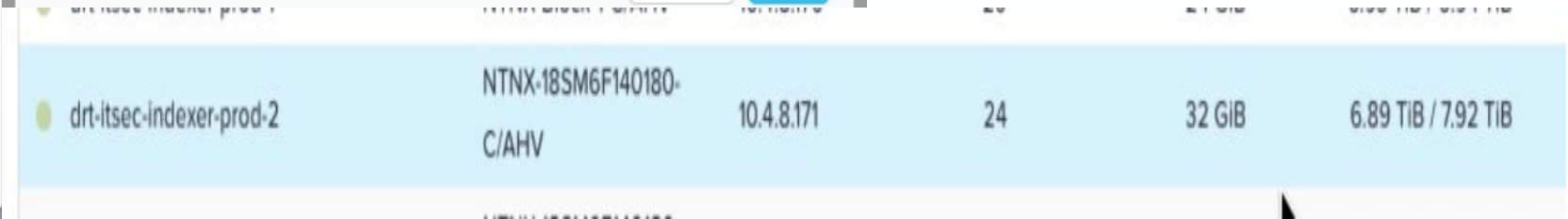


Time to Give it More Storage to Handle the New Amounts of Data: No Reboot Required









Upgrade Complete

Overview · Table

VM

VM NAME	HOST	IP ADDRESSES	CORES	MEMORY CAPACITY	STORAGE
drt-itsec-indexer-prod-1	NTNX-Block-1-C/AHV	10.4.8.170	24	32 GiB	6.95 TiB / 7.92 TiB
drt-itsec-indexer-prod-2	NTNX-18SM6F140180-C/AHV	10.4.8.171	24	32 GiB	6.9 TiB / 7.92 TiB
drt-itsec-indexer-prod-3	NTNX-18SM6F140180-A/AHV	10.4.204.24	24	32 GiB	5.7 TiB / 6.92 TiB
drt-itsec-indexer-prod-4	NTNX-Block-1-B/AHV	10.4.204.25	24	32 GiB	5.13 TiB / 6.92 TiB

Workloads Hosted On Nutanix by CyberSec Team To Date

- Splunk
- Rapid7 Console & Scanners
- OpenVAS
- Phantom
- Web Server/IPAM
- Skybox Firewall Assurance
- Intsights Threat Intel
- Exabeam UBA
- Burp Enterprise
- Fyde Zero Trust
- Kenna Security Connector
- HA Proxies
- Fos Wiki

Questions?

Automating Containment on Nutanix with Phantom

My Story

- Nick Pierini
- Manager, Security Engineering
- Splunk Phantom user for 3+ years

Nutanix Phantom App Intro

Nutanix Prism

Publisher: Nutanix

This app implements the virtualization actions for Nutanix Prism

▾ 11 Supported Actions

- **test connectivity** - Validate the asset configuration for connectivity using supplied configuration
- **get system info** - Get information about a VM
- **list vms** - Get the list of registered VMs
- **revert vm** - Revert VM to specified snapshot
- **snapshot vm** - Take a snapshot of the VM
- **start vm** - Start a stopped or suspended VM
- **stop vm** - Stop a VM
- **suspend vm** - Suspend a VM (Requires guest tools installed on vm)
- **search vms** - Query VM's based on string
- **list snapshots** - List snapshots in a cluster
- **get snapshot info** - Get information of a specific snapshot

▸ 11 Associated Playbooks

Demo

Questions